UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/710,987	08/16/2004	Makoto Izawa	27592-01101-US1	4986

30678 7590 08/13/2010

CONNOLLY BOVE LODGE & HUTZ LLP
1875 EYE STREET, N.W.
SUITE 1100
WASHINGTON, DC 20006

EXAMINER	
GELAGAY, SHEWAYE	

ART UNIT	PAPER NUMBER
2437	

MAIL DATE	DELIVERY MODE
08/13/2010	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

UNITED STATES PATENT AND TRADEMARK OFFICE

Commissioner for Patents
United States Patent and Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450
www.uspto.gov

BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

Application Number: 10/710,987
Filing Date: August 16, 2004
Appellant(s): IZAWA ET AL.

Jeffrey W. Gluck (Reg. No. 44,457)
For Appellant

EXAMINER'S ANSWER

This is in response to the appeal brief filed 06/02/10 appealing from the Office action mailed 12/21/09.

(1) Real Party in Interest

The examiner has no comment on the statement, or lack of statement, identifying by name the real party in interest in the brief.

(2) Related Appeals and Interferences

The examiner is not aware of any related appeals, interferences, or judicial proceedings which will directly affect or be directly affected by or have a bearing on the Board's decision in the pending appeal.

(3) Status of Claims

The following is a list of claims that are rejected and pending in the application:

Claims 1-2 and 4-18.

(4) Status of Amendments After Final

The examiner has no comment on the appellant's statement of the status of amendments after final rejection contained in the brief.

(5) Summary of Claimed Subject Matter

The examiner has no comment on the summary of claimed subject matter contained in the brief.

(6) Grounds of Rejection to be Reviewed on Appeal

The examiner has no comment on the appellant's statement of the grounds of rejection to be reviewed on appeal. Every ground of rejection set forth in the Office action from which the appeal is taken (as modified by any advisory actions) is being maintained by the examiner except for the grounds of rejection (if any) listed under the

subheading "WITHDRAWN REJECTIONS." New grounds of rejection (if any) are provided under the subheading "NEW GROUNDS OF REJECTION."

(7) Claims Appendix

The examiner has no comment on the copy of the appealed claims contained in the Appendix to the appellant's brief.

(8) Evidence Relied Upon

5604807	Yamaguchi et al.	02-1997
6775769	Inada et al.	08-2004
6415031	Colligan et al.	07-2002
5481610	Doiron et al.	01-1996

Keromytis et al. "Transparent Network Security Policy Enforcement" USENIX 2000, pages 1-13

(9) Grounds of Rejection

The following ground(s) of rejection are applicable to the appealed claims:

Claim Rejections - 35 USC § 103

1. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

2. Claims 1-2, 4-9 and 12-18 are rejected under 35 U.S.C. 103(a) as being unpatentable over Yamaguchi et al. (hereinafter Yamaguchi) US Patent Number 5,604,807 in view of Keromytis et al. (hereinafter Keromytis) "Transparent Network Security Policy Enforcement", USENIX 2000 and in view Inada et al. (hereinafter Inada) US 6,775,769 and in view of Colligan et al. (hereinafter Colligan) US 6,415,031.

3. As per claims 1, 5, 14 and 18:

Yamaguchi teaches a central encryption management system, comprising:

an encryption apparatus configured to be connected between a plurality of data communications terminals, (Figure 12, item 53, 54 and 55)

the encryption apparatus to perform at least one of an encrypting process or a decrypting process on data to terminate encryption-based security between communications terminals having encrypting capability and non-encrypting capability; (Figure 12, item 76) and

a manager terminal to input information into the encryption apparatus and into each of the plurality of communications terminals having encrypting capability; (Figure 12, item 51; Figure 13; col. 3, line 62-col. 4, line 20; col. 12, lines 50-64; col. 13, line 60-col. 14, line 12)

wherein the encryption apparatus further includes outputting data received on one of a plurality of ports of the encryption apparatus to another port of the encryption apparatus, after the encrypting or decrypting process is performed. (Figure 12, item 51; Figure 13; col. 3, line 62-col. 4, line 20; col. 12, lines 50-64; col. 13, line 60-col. 14, line 12)

Yamaguchi does not explicitly disclose the information including an indication of whether or not data packets are to be discarded between specific communication terminals after the data packets have been received and a time period for encryption; and wherein the encryption apparatus further includes a bridge to output data received on one of a plurality ports of the encryption apparatus to another port of the encryption apparatus, without any routing process.

Keromytis in analogous art, however, teaches a bridge to output data received on one of a plurality ports of the encryption apparatus to another port of the encryption apparatus, without any routing process. (2.1 Layer-3Filtering; 2.2 Layer-2 Filtering; 2.4 Bridge Security; 3.Bridging and IPsec) Therefore it would have been obvious to one ordinary skill in the art at the time the invention was made to modify the system disclosed by Yamaguchi with Keromytis in order to provide transparent IPsec gateway capability for a host or even a network wherein the security gateway can act as a security policy enforcer, ensuring that incoming and outgoing packets are adequately protected, based on system or network policy. (1. Introduction; Keromytis)

Both references do not explicitly disclose information including whether or not data packets are to be discarded between specific terminals after the data packets have been received. Inada in analogous art, however, discloses information including whether or not data packets are to be discarded between specific terminals after the data packets have been received. (col. 5, line 25- col. 6, line 65; col. 15, line 25-col. 16, line 56; col. 17, lines24-63) Therefore it would have been obvious to one ordinary skill in the art at the time the invention was made to modify the system disclosed by

Yamaguchi and Keromytis with Inada in order to manage the operation of the cryptographic apparatus by processing a management packet for managing the cryptographic apparatus from another machine connected to the network. (col. 17, lines 58-63; Inada)

None of the references explicitly disclose input information including a time period for encryption. Colligan in analogous art, however, discloses inputting information including a time period for encryption. (col. 8, line 7-18; col. 8, line 65-col. 9, line 5) Therefore it would have been obvious to one ordinary skill in the art at the time the invention was made to modify the system disclosed by Yamaguchi, Keromytis and Inada with Colligan in order to perform scheduling of the encryption by the encryption coordinator thereby controlling times when a particular content is scheduled to be encrypted. (col. 8, lines 11-13; Colligan)

As per claims 2 and 15:

The combination of Yamaguchi, Keromytis, Inada and Colligan teaches all the subject matter as discussed above. In addition, Yamaguchi further discloses a central encryption management system the encryption apparatus configured to receive and retransmit data in the form of encrypted data from and to one of the plurality of communications terminals having the encrypting capability, and the encryption apparatus is configured to receive and retransmit the data in the form of non-encrypted data from and to one of the plurality of communications terminals having no encrypting capability. (col. 12, lines 50-64)

As per claims 4, 6 and 16:

The combination of Yamaguchi, Keromytis, Inada and Colligan teaches all the subject matter as discussed above. In addition, Yamaguchi further discloses a central encryption management system wherein the encryption apparatus further includes a storage to store the information inputted from the manager terminal, the inputted information being used when controlling the encrypting process and the decrypting process, and the encryption apparatus controls the encrypting process and the decrypting process by comparing the information stored in the storage with header information of a data packet of the data received through one of the plurality of ports. (col. 11, line 44-col. 12, line 45)

As per claim 7:

The combination of Yamaguchi, Keromytis, Inada and Colligan teaches all the subject matter as discussed above. In addition, Yamaguchi further discloses a central encryption management system wherein the information comprises at least one of information associated with the presence or absence of encryption or decryption process, the availability of packet communications, an encryption level, a time period to perform encryption, a encryption policy or an encryption key. (Figure 12, item 51; Figure 13; col. 3, line 62-col. 4, line 20; col. 12, lines 50-64; col. 13, line 60-col. 14, line 12)

As per claim 8:

The combination of Yamaguchi, Keromytis, Inada and Colligan teaches all the subject matter as discussed above. In addition, Inada further discloses wherein the at least one of the plurality of communications terminals are inside a secured network. (Figure 12)

As per claim 9:

The combination of Yamaguchi, Keromytis, Inada and Colligan teaches all the subject matter as discussed above. In addition, Inada further discloses wherein the at least one of the plurality of communications terminals is outside secured network. (Figure 12)

As per claim 12:

The combination of Yamaguchi, Keromytis, Inada and Colligan teaches all the subject matter as discussed above. In addition, Yamaguchi further discloses a central encryption management system wherein the plurality of communications terminals are arranged in a plurality of local area networks. (Figure 12, item 51; Figure 13; col. 3, line 62-col. 4, line 20; col. 12, lines 50-64; col. 13, line 60-col. 14, line 12)

As per claim 13:

The combination of Yamaguchi, Keromytis, Inada and Colligan teaches all the subject matter as discussed above. In addition, Yamaguchi further discloses a central encryption management system wherein comprising a plurality o f manager terminals, each of the plurality o f manager terminals to manage encryption and decryption settings in the communications terminals having encrypting capabilities in at least one of the plurality of local area networks. (Figure 12, item 51; Figure 13; col. 3, line 62-col. 4, line 20; col. 12, lines 50-64; col. 13, line 60-col. 14, line 12)

As per claim 17:

The combination of Yamaguchi, Keromytis, Inada and Colligan teaches all the subject matter as discussed above. In addition, Keromytis further discloses performing

an encrypting process or a decrypting process on data received at one of the plurality of ports after passing through a data link layer and a physical layer; and outputting encrypted or decrypted data from another of the plurality of ports through a data link layer and a physical layer associated with the other port without passing said data to a network layer in which routing between networks are controlled. (2.1 Layer-3Filtering; 2.2 Layer-2 Filtering; 2.4 Bridge Security; 3.Bridging and IPsec)

4. Claims 10-11 are rejected under 35 U.S.C. 103(a) as being unpatentable over Yamaguchi et al. (hereinafter Yamaguchi) US Patent Number 5,604,807 in view of Keromytis et al. (hereinafter Keromytis) "Transparent Network Security Policy Enforcement", USENIX 2000 and in view Inada et al. (hereinafter Inada) US 6,775,769 and in view of Colligan et al. (hereinafter Colligan) US 6,415,031 and in view of Doiron et al. (hereinafter Doiron) US 5,481,610.

As per claim 10:

The combination of Yamaguchi, Keromytis, Inada and Colligan teaches all the subject matter as discussed above. None of the combination cited explicitly disclose wherein the encryption apparatus comprises a data path for a connected terminal and performs the encryption process or the decryption process on data received or transmitted on each data path using a different encryption key associated with the connected terminal. Doiron in analogous art, however, discloses wherein the encryption apparatus comprises a data path for a connected terminal and performs the encryption process or the decryption process on data received or transmitted on each data path using a different encryption key associated with the connected terminal. (col. 7, line 29-

col. 8, line 33) Therefore it would have been obvious to one ordinary skill in the art at the time the invention was made to modify the system disclosed by Yamaguchi, Keromytis and Inada and Colligan with Doiron in order to protect the data path by preventing signal analysis thereby avoiding revealing the cryptographic keys. (col. 8, lines 21-23; Doiron)

As per claim 11:

The combination of Yamaguchi, Keromytis, Inada and Colligan teaches all the subject matter as discussed above. None of the combination cited explicitly disclose wherein the encryption apparatus comprises wherein the plurality of communications terminals having encrypting capability are connected to the encryption apparatus through an access point. Doiron in analogous art, however, discloses wherein the encryption apparatus comprises wherein the plurality of communications terminals having encrypting capability are connected to the encryption apparatus through an access point. (col. 3, lines 3-35) Therefore it would have been obvious to one ordinary skill in the art at the time the invention was made to modify the system disclosed by Yamaguchi, Keromytis, Inada and Colligan with Doiron in order to provide a secure radio frequency communications system that encrypts and decrypts messages. (col.1, lines 5-10; Doiron)

(10) Response to Argument

Appellant argues that independent claims 1, 5, 14 and 18 all contain elements that are not disclosed or suggested by the combination of the cited references. Specifically, Appellant argues that “there is no nexus between the "management

packet" any information regarding the discarding of information/packets, i.e. there is no showing or discussion in Inada et al. that establishes that such a “management packet” contains such information. Therefore, at least this portion of Inada et al. fails to teach that the cryptographic apparatus receives from a manager terminal “information for instructing whether or not data packets are to be disclosed between the specific communications terminals after the data packets have been received” as claimed.

Inada teaches a cryptographic apparatus for relaying data between a plaintext network and a ciphertext network. (figure 1, col. 2, lines 36-38) Inada teaches configuration of a cryptographic apparatus adopting a repeater that can be installed without changing the network parameters of the existing machines on a network (i.e. "a repeater-type cryptographic apparatus”) processing information addressed to the home station, transmitted as a packet, for example, a management packet for managing the repeater-type cryptographic apparatus, or the like. (col., 5, lines 16-28)The ciphertext output filter is a filter for a packet transferred to the ciphertext port for determining the packet to be discard packet which need not be transmitted from the ciphertext port. (col. 5, lines 60-63) A management packet for managing the repeater-type cryptographic apparatus, etc., can be processed and the operation of the repeater-type cryptographic apparatus can be managed as another machine changing setting of cryptographic processing of the repeater-type apparatus. (col. 14, lines 5-10)

As set forth above, Inada teach receiving a management packet for managing and setting a cryptographic apparatus with different functionalities which includes determining the packet to be a discard packet which need not be transmitted.

Examiner notes that Applicant has provided Martin-Flatin and Znary (see page 11) to show many networks include management functionality performed among peer systems. Examiner would like to point out that the terminal that sends the "management packet" whether among peers or centralized is considered the "manager terminal".

Appellant further argues (see page 12) even if, arguendo, Inada did teach or suggest the claimed “management terminal,” and even if the “management packet” of Inada et al. were sent by the management terminal, the cited portions of Inada et al. fail to establish the “management packet” contains “information for instructing whether or not data packets are to be discarded between specific communication terminals after the data packets have been received.”

Appellant argues that Colligan refer to the encryption of information in a video-on demand source and discuss scheduling of encryption and the use of an encryption key based on "an appropriate time epoch" ...nowhere is there any discussion of providing "a time period for encryption" as claimed. Colligan teaches loading a digital video content from the content source to the encryption coordinator wherein the scheduling of the encryption is performed by the encryption coordinator under control of the content manager. The content manager holds the schedule information regarding the times when a particular content is scheduled to be encrypted. Colligan clearly teaches a time period for encryption (i.e. times when a particular content is scheduled to be encrypted).

Appellant argued that what is recited includes "a manager terminal to input information into the encryption apparatus and into each of the plurality of communications terminals having encrypting capability, the information including

whether or not data packets are to be discarded between the specific communication terminals after the data packets have been received and a time period for encryption."

Yamaguchi et al. teaches a cipher communication system and scheme capable of realizing the cipher communication without affecting the already existing application programs and hardware, and establishing a synchronization at the start and end of the cipher communication. In particular, Yamaguchi discloses wherein each client 53 and each cipher gateway device 54 are connected with the key distribution center 51 (i.e. manager terminal), the network 52, and the server 55.3 . A session key is distributed from the key distribution center 1 to each terminal.(figure 12, col. 6, lines 62-65) The key distribution center 51 generates the session key and transmits the generated session key to the client 53 and the cipher gateway device54 through the network 52 while session between the client 53 and the server 55 is established through the network 52 and the cipher gateway device 54. (col. 9, lines 2-7) Therefore, Yamaguchi teaches a manager terminal (i.e. key distribution center 51) to input information into the encryption apparatus (i.e. distribute session key to cipher gateway device). Yamaguchi does not explicitly disclose the information including an indication of whether or not data packets are to be discarded between specific communications terminals after the data packets has been received and a time period for encryption. However, Inada teaches setting up a cryptographic apparatus for relaying data between a plaintext network and a ciphertext network. (figure 1, col. 2, lines 36-38) Inada teaches managing the cryptographic apparatus with a management packet with different operations one of which is to determine whether or not to discard a packet. (see discussion above)

The combination of Yamaguchi and Inada teaches "a management terminal to input information into the encryption apparatus and into each of the plurality of communications terminals having encrypting capability, the information including an indication of whether or not data packets are to be discarded between specific communication terminals after the data packets have been received. Both references do not explicitly disclose input information including a time period for encryption. Colligan in analogous art, however, discloses inputting information including a time period for encryption. (col. 8, line 7-18; col. 8, line 65-col. 9, line 5) Therefore it would have been obvious to one ordinary skill in the art at the time the invention was made to modify the system disclosed by Yamaguchi and Inada with Colligan in order to perform scheduling of the encryption by the encryption coordinator thereby controlling times when a particular content is scheduled to be encrypted. (col. 8, lines 11-13; Colligan)

In response to applicant's arguments against the references individually, one cannot show nonobviousness by attacking references individually where the rejections are based on combinations of references. See *In re Keller*, 642 F.2d 413, 208 USPQ 871 (CCPA 1981); *In re Merck & Co.,* 800 F.2d 1091, 231 USPQ 375 (Fed. Cir. 1986).

(11) Related Proceeding(s) Appendix

No decision rendered by a court or the Board is identified by the examiner in the Related Appeals and Interferences section of this examiner's answer.

For the above reasons, it is believed that the rejections should be sustained.

Respectfully submitted,

/Shewaye Gelagay/

Examiner, Art Unit 2437

Conferees:

Emmanuel Moise
/Emmanuel L. Moise/
Supervisory Patent Examiner, Art Unit 2437

Michael Pyzocha
/Michael Pyzocha/
Primary Examiner, Art Unit 2437